This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

THIS PAGE BLANK (USPTO)

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : G06F 1/00 — A1

(11) International Publication Number: WO 93/06542

(43) International Publication Date: 1 April 1993 (01.04.93)

(21) International Application Number: PCT/NL92/00161

(22) International Filing Date: 21 September 1992 (21.09.92)

(30) Priority data:
9101594 20 September 1991 (20.09.91) NL

(71) Applicant *(for all designated States except US)*: TRES AUTOMATISERING B.V. [NL/NL]; Industrieweg 161, NL-3044 AS Rotterdam (NL).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)* : DE BOER, Dick, Peter [NL/NL]; Rubenslaan 8a, NL-3116 BN Schiedam (NL). VAN DEN HONDEL, Johannes [NL/NL]; Vlaardingerdijk 233, NL-3117 EN Schiedam (NL).

(74) Agent: SCHUMANN, Bernard, Herman, Johan; Arnold & Siedsma, Sweelinckplein 1, NL-2517 GK The Hague (NL).

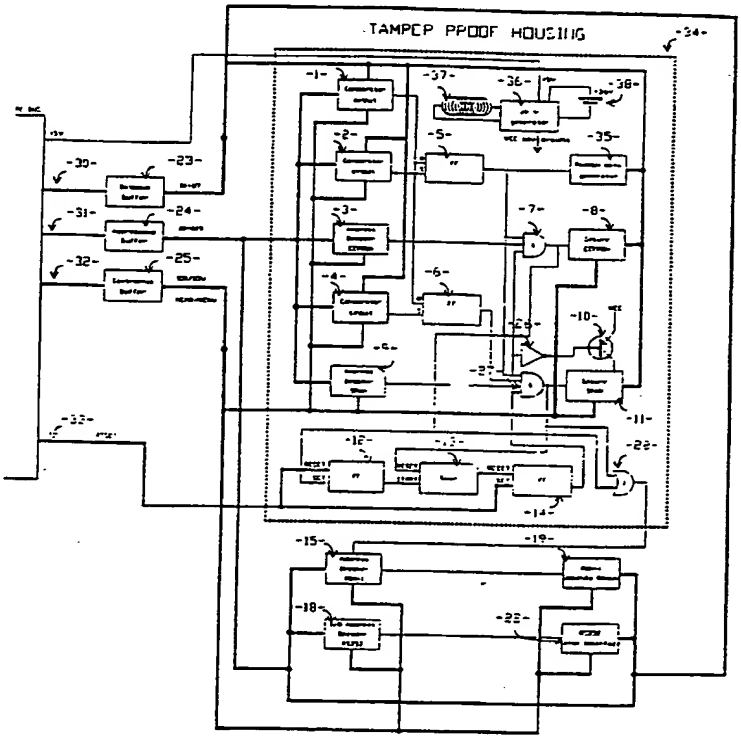
(81) Designated States: AU, BB, BG, BR, CA, CS, FI, HU, JP, KP, KR, LK, MG, MN, MW, NO, PL, RO, RU, SD, UA, US, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, SN, TD, TG).

Published
With international search report.
In English translation (filed in Dutch).

(54) Title: COMPUTER SYSTEM WITH SAFEGUARDING

(57) Abstract

The invention relates to a protection means for personal computers which at machine level and independently of the operating system protects the personal computer and the software and information situated thereon against unauthorized use, irrespective of the fact of whether this personal computer is used as stand-alone device or whether this personal computer is incorporated in a data communication network. The protection means consists on the one hand of an electronics board provided with printed circuits and electronic circuits consisting of ICs (integrated circuits) and electronics related thereto which together form a plug-in card which is provided with contact surfaces for input and output of information, and on the other hand of software which is stored in information carriers which per se form a component of the electronics on the plug-in card, with the object of granting access to the personal computer and the information stored thereon as well as the coding and decoding of this information after the specific conditions for obtaining access have been fulfilled.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	FI	Finland	MN	Mongolia
AU	Australia	FR	France	MR	Mauritania
BB	Barbados	GA	Gabon	MW	Malawi
BE	Belgium	GB	United Kingdom	NL	Netherlands
BF	Burkina Faso	GN	Guinea	NO	Norway
BG	Bulgaria	GR	Greece	NZ	New Zealand
BJ	Benin	HU	Hungary	PL	Poland
BR	Brazil	IE	Ireland	PT	Portugal
CA	Canada	IT	Italy	RO	Romania
CF	Central African Republic	JP	Japan	RU	Russian Federation
CG	Congo	KP	Democratic People's Republic of Korea	SD	Sudan
CH	Switzerland			SE	Sweden
CI	Côte d'Ivoire	KR	Republic of Korea	SK	Slovak Republic
CM	Cameroon	LI	Liechtenstein	SN	Senegal
CS	Czechoslovakia	LK	Sri Lanka	SU	Soviet Union
CZ	Czech Republic	LU	Luxembourg	TD	Chad
DE	Germany	MC	Monaco	TG	Togo
DK	Denmark	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	US	United States of America

Computer-system with safeguarding

The invention relates to a protection means for personal computers which at machine level and independently of the operating system protects the personal computer and the software and information situated thereon against unauthorized use, irrespective of the fact of whether this personal computer is used as stand-alone device or whether this personal computer is incorporated in a data communication network.

The protection means consists on the one hand of an electronics board provided with printed circuits and electronic circuits consisting of ICs (integrated circuits) and electronics related thereto which together form a plug-in card which is provided with contact surfaces for input and output of information, and on the other hand of software which is stored in information carriers which per se form a component of the electronics on the plug-in card with the object of granting access to the personal computer and the information stored therein as well as the coding and decoding of this information after the specific conditions for obtaining access have been fulfilled.

Using such a plug-in card the functionality of a personal computer can be enlarged. By inserting this plug-in card into one of the expansion bus connections which are situated on the motherboard of the personal computer and are per se embodied with contact surfaces for the input and output of information which have a one-to-one relation with the contact surfaces on the plug-in card, the functionality present on the plug-in card is added to the functionality of the personal computer. A significant part of the electronic circuits on the plug-in card for the protection means is contained in an opaque, tamper-proof housing which prevents vital signals of the protection means being tapped, by-passed or disconnected and which makes the information held in the

BNSDOCID: <WO 9306542A1 I >

information carriers situated inside the tamper-proof housing inaccessible to unauthorized persons.

Placed on the plug-in card are information carriers which contain the required software and control data of the protection means in addition to identification and coding keys which are needed to enable the electronics to operate with the information which is coded by the protection means on the basis of the coding keys and which is stored on the peripheral equipment coupled to the personal computer.

Also coupled to the protection means are user keys on the basis of which a user does or does not obtain access to the personal computer and the software and information stored thereon.

Depending on the required degree of confidentiality demanded of user and system keys, these keys can be stored on the personal computer itself in the form of passwords, or they can be stored in an external information carrier such as for example a chip card.

Such a chip card is known from the article "Smart Card" by A.J. Selezneff in "Philips Telecommunications and Data Systems Review", volume 45, no.4, December 1987.

The chip itself (also called "integrated circuit") is placed on a printed circuit film, wherein the circuit film has contact surfaces for input and output of data. The integrated circuit and the circuit film are arranged as an entity in a plastic envelope. The integrated circuit comprises inter alia a data memory which can serve among other things to store data such as PIN-code, encryption keys etc., one of the characteristics of which is that the chip card blocks itself after a number of attempts have been made to gain access to the information stored on the chip card and wherein the conditions set by the intelligence of the chip card have not been met. This external information carrier is read by means of a read/write unit coupled to the personal computer and into which this external information carrier is introduced. The rest of this document assumes a situation in which a chip card is used as external information carrier for the purpose of personal computer protection.

BNSDOCID: <WO 9306542A1 >

The manner in which the key control for the protection is realized is not in itself relevant for the operation of the plug-in card but it does however increase the effectiveness of the protection means.

In order to control access to an external information carrier such as for instance a chip card, use can be made of different methods. This may for instance be in the form of a PIN-code which must be entered by the user or in the form of a signature if use is made of signature recognition equipment, or in the form of a fingerprint if use is made of fingerprint recognition equipment, or in the form of optical control information, for example inspecting the iris by means of optical laser equipment.

The operation of the plug-in card must be envisaged as follows. By inserting the plug-in card in one of the expansion bus connections of the personal computer the protection means becomes a component of the functionality of this personal computer which is available to the user or users of this personal computer. If a person wishes to make use of this personal computer, he must first enter a code in one of the above specified ways, on the basis of which a check is made by the plug-in card as to whether this code gives authorization to work with this personal computer and the information stored thereon. If this is the case, the functionality of this personal computer is then made available to him or her so that work can be performed in the normal manner.

The information which is read from and written to the peripheral devices of the personal computer by this user with this personal computer is automatically decoded and coded by the plug-in card on the basis of keys which are known only to the plug-in card.

By means of coding of the information, which is done by the plug-in card during writing of information, this information is provided with unique characteristics whereby this information can only be used together with the plug-in card with which this information is coded.

The plug-in card also ensures that information based on an algorithm which is known only to this specific plug-in

BNSDOCID: <WO _ 9306542A1 I >

card is written to physical locations (addresses) on the peripheral equipment other than those which are designated by the software operating on this personal computer, which effectively means that this peripheral equipment cannot be read by any other device, or by a device equipped with another plug-in card, since this will approach the information on the peripheral equipment with a different algorithm and the result thereof will therefore be unpredictable. As the information written onto the peripheral devices using the plug-in card and the plug-in card itself are inextricably linked with one another, only this specific combination will lead to the desired result.

Comparable existing products

Protection means for the personal computer are known from the literature which protect personal computers in similar manner. These provide however only a very limited protection since they function at software level as an extension of the operating system. No integration therefore takes place between the protection means and the hardware of the personal computer itself. Reference is made here to products such as Disklock from IRIS, Safetools from SOFTECH, DialockBoot from COM&DIA, Watchdog from FISCHER, Certus from FONDATION WARE and AuthentICC from Bull CP8.

The drawbacks associated with these known protection products are that the protection software is supplied as a normal program (also known as driver) which must be installed on the hard disc. When the personal computer is started up this protection program is loaded just as any other program by the operating system and made active as for instance a so-called "TSR-Program" (Terminate and Stay Resident Program).

This type of protection means is therefore an additional function (an extension) of the operating system and not an additional function of the machine. Such protection means will not therefore become a component of the machine. This type of protection software is comparatively simple to translate from machine code to program code that is once again readable, whereafter the operation of the program

is known and can even be extended with individual routines to extract coded information from the computer. These protection means can further be switched off and/or by-passed with comparatively simple means, whereafter the information can be examined with all kinds of standard auxiliary means and possible encryptions of information and programs on the hard disc for instance can be rendered inoperative in comparatively simple manner, for example by monitoring the information being processed by the protection program. In this way a confidential coding key, for instance, with which the information on for instance a hard disc is coded can be obtained and the protected information decoded in simple manner without any in-depth knowledge relating to the operation of the protection means being required.

Because this type of protection means functions together with one particular operating system, usually the MS DOS operating system, whether or not the protection means can be used is determined by the choice of operating system. Even the implementation of a new version of the same operating system than for which the protection means has been developed can cause problems in the use of such a protection means. Operation with the protection means and an operating system other than that for which this protection means is developed is not possible. Work can only be done with other operating systems without this protection means and the information and software cannot therefore be protected against fraudulent use.

It is frequently the case, certainly on the personal computer, that work is done with different operating systems on physically the same peripheral equipment, such as for instance a hard disc.

If use is made of the above described protection means, protection is only provided for a part of the information stored on the peripheral devices, namely the part controlled by the operating system for which the protection means has been developed.

Since this type of protection means does not work together with other operating systems the information processed with these other operating systems cannot be protected in

BNSDOCID: <WO__9306542A1_I_>

any way by this protection means and can be approached and used or misused by anyone. In other words, the range within which such protection means operate is exceptionally limited in relation to the possibilities offered by the equipment and the software obtainable therefor.

The object of the invention is to provide a protection means for personal computers which can function at all times at machine level wholly independently of operating system and/or brand of personal computer without therein impinging upon facilities present in the machine and wherein the drawbacks and limitations of the above described protection methods are eliminated.

This object is achieved by supplying the protection means not as a normal program that must be loaded in the usual manner by an operating system of the personal computer but by integrating it into the equipment at hardware level by means of a plug-in card and arranging thereon all facilities required for the protection means. (See figure 6 for a symbolic representation of what this plug-in card could look like).

The protection program is structured in hardware form in one or more volatile or non-volatile information carriers -61-, wherein parts of the protection hardware are likewise protected by electronics on the same plug-in card against sabotage or unauthorized operations. These electronics are built into a so-called "tamper-proof housing" -65-. By means of the address decoders -63- and -64-, memory and communication port can be fitted onto an address in the machine that is still free. Using the communication port -62-which is connected to board connector -66- a read/write unit -67- can be coupled via the cable -70-, with which unit an external information carrier -68- can be read or written to. The external information carrier can for instance be used for storing confidential information such as user and system keys and similar information. Using the Bus Board Connector -69- the plug-in card is coupled to the bus of the machine and the memories on this plug-in card can be accessed via the data bus -26- and the address bus -28-. The protection means

thus effectively becomes a component of the machine which, in respect of the vital parts such as the information carriers, for instance discs and tapes etc., can no longer function without the protection means because unique characteristics are coupled by the protection means to these information carriers which can no longer be detached therefrom.

Only by destroying the information recorded on these information carriers or by de-installing (removing) the protection means by means of special software via a user (system controller) specially authorized therefor can these information carriers be re-used without the protection means.

The protection means can only be installed and removed making use of a special key, the system controller key which, like the user keys, is likewise recorded for instance on an external information carrier.

Only with this special key can the protection means be installed onto the machine and activated or deactivated and removed. This special key is also required to assign to the users of the machine rights which are stored in for instance the external information carrier in which the user keys of this user are also stored, with respect to the use of the machine and the peripheral devices coupled thereto.

This protection means also provides an effective manner of securing against unauthorized copying of software without the users of this software experiencing any inconvenience therefrom or the developers of this software having to take account of this in the production and development of their software.

An installed package is coupled by the protection means to one particular combination of personal computer with protection means.

The only requirement for this purpose that the software distributor has to fulfil is that the "master distribution means" for this software must be manufactured with machines that are equipped with the invention and an external information carrier necessary for installing the software must be added to the package. The production and distribution process proceeds further as was the case before. On which

BNSDOCID: <WO__9306542A1_I_>

computer the software is installed is recorded in code on the distribution diskette on the basis of keys.

Installation of the software can only take place on machines provided with a protection means and equipped with special software for installation which forms part of the protection means. Installing of this software on for instance the hard disc takes place in a manner such that it is only usable on the computer on which the official installation has taken place. The number of installations on this specific computer is unlimited, but installation is not permitted on another machine until the software on the other computer is de-installed by means of a special procedure, whereby the installation medium is released for installation on another machine. In this way authorized installations can be permitted on one or more machines in simple manner.

A PC protection means is thus obtained which under all conditions protects in an effective and adequate manner against undesired infringement in those areas where criminal elements could take advantage and/or cause damage to companies and/or individuals, namely with the information and software stored on the personal computer and which in respect of the use of the protection means is wholly transparent and therefore requires no special actions whatever by the user.

Operation and advantages of the invention

(general)

The invention and its advantages will now be elucidated with reference to the following drawings, in which:

figure 1 shows a schematic view of the hardware functionality for the protection means present on the plug-in card;

figure shows a block diagram relating to the installation of the plug-in card;

figure 3 shows a block diagram relating to the initialization of the plug-in card;

figures 4a and 4b show block diagrams relating to the functionality contained in the **"Basic protection part"** of the plug-in card;

figure 5 shows a block diagram relating to the

BNSDOCID: <WO 9306542A1 | >

functionality contained in the **"Encryption/Decryption part"** and **"Access Control part"** of the plug-in card; figure 6 is a symbolic representation of the plug-in card.

The diagram in figure 1 represents a number of functions which are arranged on the plug-in card, wherein "-16-" serves as one or more program memories. These may be volatile or non-volatile memories. Included herein are respectively the **"Basic protection"**, the **"Encryption/Decryption"** and the **"Access Control"** functions.

These are program parts which, after they have been arranged and reported, are inextricably linked to the plug-in card and the peripheral devices of the computer. A part of the protection means is also arranged during installation in coded form in the memory -8- which is accommodated in a so-called tamper-proof housing. The unchanged presence of the software is monitored at set times by the protection means itself during operation with the protection means. As briefly stated above, the vital functions of the protection software are included in non-readable code in the information carrier -8-. When the machine is switched on these program parts are decoded on the basis of special keys into readable code, after an authorized user has started up (switched on) the system, and are placed in the memory -11- which also serves as working memory for the protection means.

Provisions are made by the protection means which ensure that entering and reading of information proceeds via the protection means at all times. Only then can the protection of machines and information be guaranteed. The connections made to the existing hardware and firmware for the purpose of the protection are regularly monitored as to their integrity. In other words: if these connections still exist, are these connections still present in unchanged form, has no attempt been made to extract vital information from the protection means in unauthorized manner, such as for instance protection keys and program information which are stored in the memories situated inside the tamper-proof housing.

BNSDOCID: <WO__9306542A1_I_>

N.B. By firmware must be understood programs or program parts which are accommodated for instance in a ROM (Read Only Memory) and which form, as it were, a fixed component of a machine and which do not disappear when the energy supply to the machine is discontinued.

These checks are performed by both the protection software and the electronics on the plug-in card. If unauthorized alterations are detected in the protection means the system will report this, a record is made of the user who performed these actions, access for this user is temporarily blocked and only reinstated when the steps (protocol) required for this purpose have been performed. The operation of the machine is also stopped at a point such that no sensible conclusion can be drawn therefrom, whereafter further working with the machine is no longer possible without restarting it (turning off and switching on again).

Operation and advantages of the invention

(Tamper-proof housing)

On the plug-in card a number of circuits and information carriers is arranged in a tamper-proof housing which has the object of protecting the information carrier or carriers accommodated therein against unauthorized actions such as reading and/or altering thereof or against executing of the software that is present therein at a particular moment.

This tamper-proof housing -34- is shown schematically in figure 1. The object thereof is to create a sector in which program code can be loaded and executed and which can contain the keys necessary for the protection without it being possible to influence this information from outside other than by following a stringent protocol wherein a number of electronic and program conditions have to be met, wherein the sequence in which the required actions have to be performed also determines whether the electronics incorporated therein will function or not. If the set conditions are not fulfilled the electronics arranged in the tamper-proof housing will then block the machine. It is not possible to determine from outside by means of a "trial and

error" method what the conditions are that have to be fulfilled to gain access to the functionality contained in the tamper-proof housing, since at the first attempt undertaken to do so the personal computer immediately blocks in a manner such that work can no longer be carried out therewith other than by restarting the machine (turning off and switching on again).

By means of the "Reset" signal, which is made active on the reset line -32- by the normal electronics of the machine when the machine is started, a condition is created by the electronics in the tamper-proof housing which enables the protection means to be initialized (made ready for normal processing). This results in setting of a once-only condition wherein the memory -11- arranged in the tamper-proof housing is accessible under special conditions. At that moment the memory -11- still does not contain any relevant information that could be of use to a "hacker", this is only present after the initialization of the protection means.

The conditions required to approach the memories arranged in the tamper-proof housing after initialization can only be set by addressing -19- in a specific manner and by performing a fixed series of instructions in relation to the address where -19- is placed with the address decoder -15-. This condition, which is checked by the electronics accommodated in the tamper-proof housing, is set such that it cannot be created in a manner other than that prescribed by the electronics of the protection means. The memory -8- cannot be made accessible in any other manner whatsoever.

In order to approach memory -11- this process must be repeated however at addresses which lie within the range of memory -8-. When memory -8- is made active for the first time, this then results in the starting of the independent timer -13-.

Timer -13- ensures that the protection means must be addressed, for instance every 55 milliseconds. If this does not happen the machine is blocked against further processing. To approach the memories -8- and -11- the following conditions must be fulfilled:

For -8-: 1. A number of instructions must be performed

from -16- from a fixed address. That this actually takes place is checked by -2-, which makes -5- active when all conditions have been fulfilled.

2. The correct address must be placed by the processor at the address bus -28-, which is likewise monitored by -2-. The performing of the required series of instructions cannot therefore take place from any location other than from -16- on the plug-in card, which is an imperative condition which guarantees that this condition cannot be set by means of another program and also guarantees that the operation is transferred to the electronics accommodated in the tamper-proof housing.

2. The FlipFlop -14- must be active as this is one of the conditions which activate the "AND" gate 27. This is set by an independent timer -13- which is a component of the electronics accommodated in the tamper-proof housing and which must be reset for instance every 55 milliseconds. If this does not occur the voltage is removed from -11-, whereby the information in -11- is effectively erased instantaneously and -8-and -11- are disconnected from the address bus -28- whereby they can no longer be approached. They can only be made available again by physically turning off and switching on the machine again or by generating a so-called hard reset, whereby the plug-in card is initialized once again. The hard reset is usually a switch which is arranged on the machine and which has essentially the same effect resulting from turning off and switching on the machine again. Herewith can be guaranteed that within the time made available for this purpose by the timer -13- the protection means is activated and the checks can be performed which guarantee the integrity of the protection means.

Only these three conditions together activate -7- whereby -8- becomes accessible and whereby flipflop -12- is set, which in turn starts the timer -13-, whereafter the memories

BNSDOCID: <WO 9306542A1 I >

accommodated in the tamper-proof housing must be made active within the time timer -13- makes available therefor, as otherwise the system is blocked against further processing.

For -11-: 1. Herefor, all the preceding conditions required for approaching -8- must first be fulfilled.

2. Specific addresses which lie within the range of memory -8- and which cannot be in any way deduced must once again appear at the address bus -28-, this being checked by -4-.

3. A particular series of instructions must be performed at that address, which is likewise checked by -4-, and which cannot be performed in any way whatever from another location in order to fulfil this condition.

Only if these conditions are fulfilled is -20- activated, which in turn makes -11- accessible, which results in the independent timer -13- being reset, with the understanding that the whole time of -13- is once again made available.

The software required for the vital functions of the protection means is stored in coded form in the memory -8-. In the initialization phase of the machine and the plug-in card this software is decoded on the basis of a key read from the external information carrier together with a key included in -8- and placed in the information carrier -11-. This is therefore an action which only takes place if it is performed by authorized users, since only they have at their disposal a valid key for decoding the software from -8- to -11-.

If any attempt is made to take over control of the electronics accommodated in the tamper-proof housing and in this way extract information from the memories accommodated therein, the energy supply of -11- is cut by means of -10-, on the basis of timer -13-, within the time which timer -13- makes available therefor, in that -14- is deactivated by -13- which effectively means that the information recorded in -11- such as keys and software is instantaneously erased.

The sole way to prevent this is to give control to the electronics accommodated in the tamper-proof housing within

the time which timer -13- makes available for this purpose. This monitors first of all whether the checks required for the protection can still be performed and/or whether all conditions are met for the protection. If this is not the case, the energy supply is likewise cut from -11- in the above described manner and the machine blocked against further processing.

As the only way to make the memories inside the tamper-proof housing accessible is to perform several series of fixed instructions at required addresses, the start-up of the software present in the memories accommodated in the tamper-proof housing can be guaranteed. This is in fact the sole manner in which timer -13- can be re-started and the only way of preventing the machine being blocked due to exceeding of the time made available by timer -13- for activating the electronics in the tamper-proof housing.

The software accommodated in the memories -8- and -11- provides a number of checks which guarantee that the paths which must be followed within the machine in order to be able to guarantee the protection thereof are also followed. These checks take place for the following couplings:

1. Dealing with the interrupt of the clock of the machine, the timer interrupt, INT 08. This is generated ± 18 times a second by the clock chip of the computer itself.

This is also referred to as the "timer tick". The frequency at which this timer tick is generated is normally 55 milliseconds, but this frequency can be altered as required. Assuming the normal situation, this means that every 55 milliseconds a timer tick is generated by the machine itself, on the basis of which a number of operations must be performed.

This signal is also required for actuating timer -13- which is accommodated in the tamper-proof housing and which thus functions as a "watch-dog" for the above mentioned timer interrupt. If this signal does not arrive, the energy provision of -11- is discontinued in the above specified manner and the information in -11-

BNSDOCID: <WO 9306542A1 I >

is instantaneously erased and further processing of the machine blocked.

Dealing with the timer interrupt is coupled to a program connection with software in the memories accommodated in the tamper-proof housing. This connection is checked for integrity at each timer tick. Should this connection no longer be reliable, the energy supply of memory -11- is discontinued whereby the information therein is immediately erased and the processing of the machine blocked.

2. The input from the keyboard is also controlled via software accommodated in the memories -8- and -11-. This connection is also checked every timer tick. Also in the case this connection no longer meets the set requirements the information in -11- is erased in the above described manner and the machine blocked against further processing.

3. In addition, all read and write actions which take place for the hard disc are controlled by software accommodated in the memories -8- and -11-. This connection is also checked at each timer tick and, in the case of irregularities, blocked in the above described manner. It is also impossible without this function and the keys associated therewith to use the information held on the peripheral equipment of the machine due to the coding of that information.

If desired an individual microprocessor can be accommodated in the tamper-proof housing, whereby it can be guaranteed that vital information inside the machine such as user keys and the like appear only once at the data bus -26- and whereby the possibility is created of executing protection software inside the tamper-proof housing.

The tamper-proof housing is safeguarded against opening thereof by means of -22-, -24- and -23-, which have the following operation:

-24- is wiring which is arranged as reinforcement in the tamper-proof housing over the whole surface of the housing in a manner such that any attempt made to

remove this housing has the consequence that this wiring, which serves as a switch, is interrupted. When this wiring forms an uninterrupted whole the (+5V) is connected through directly via a circuit in -22- to the VCC of all circuits situated in the tamper-proof housing.

If this wiring is broken the normal (+5V) is discontinued by -22- and a much too high voltage is briefly applied to the VCC to all these circuits which has the effect of burning through these circuits which will thereby no longer be usable. It is thereby also no longer possible to determine in any way whatever the operation of these circuits with the purpose of reconstructing the electronic circuits situated inside the tamper-proof housing;

-22- contains the electronics with which this high voltage is built up using the energy supplied from a battery -38- and with which the closed connection of -24- is constantly monitored;

-23- is a high-grade energy cell which is likewise located inside the tamper-proof housing and which cannot be disconnected or replaced from outside. This energy cell is charged during normal use of the machine by means of electronics accommodated in -22- and energy supplied externally.

By incorporating the wiring in the tamper-proof housing the opening thereof without damaging the wiring has become almost humanly impossible. Should efforts be undertaken to open the housing, whereby the wiring inside the housing is unavoidably damaged, high voltage generator -22- is set into operation, which applies this high voltage for a short time to the components located inside the tamper-proof housing, whereby these components become wholly unusable and it is no longer possible to determine in any way whatever what the operation or lay-out was of these circuits which were formed by these components.

The plug-in card is also provided with a device

constructed from electronic circuits which has the object of disturbing capture of the information being exchanged over the data bus -26- of the machine between the plug-in card and the machine with random (RANDOM) information so that, should this information be captured in order to thus extract information from the protection means, no unambiguous conclusions can be related thereto due to the disturbance of the random information which takes place at random moments in time and with random quantities.

A great advantage of the lay-out of the plug-in card is that, despite the software which serves in -16- and -8- as firmware on the plug-in card, the distribution of new versions thereof can take place by sending a coded diskette which can be loaded with special software without the user being confronted with all kinds of operations involving changing of components on the plug-in card.

This advantage is achieved by embodying both -16- and -8- as a so-called EEPROM (Electrically Erasable Programmable Read Only Memory) which, in contrast to an EPROM (Erasable Programmable Read Only Memory), can be erased with voltage and does not need a UV light source for erasing as is the case with EPROM.

In other words, an EEPROM can, as it were, be treated as normal memory in respect of reading and writing thereof, with the understanding that the information is not erased at the moment energy is no longer being supplied to the EEPROM, in which respect the EEPROM functions as an EPROM and not as normal memory.

Operation and advantages of the invention

(installation figure 2)

The installation procedure is shown in figure 2 with reference to a block diagram. A check is first made in -33- as to whether the protection means is already installed. If this is the case, a jump is made to figure 3, -40- to check if the protection means is already initialized. We shall return to this later in **Operation and advantages of the invention** (initialization)

It can be seen in -34- of this block diagram that a general protection key is read from an external information carrier after a check has been made whether this external information carrier fulfills all requirements and specifications.

If this is not the case, a jump is made to -39-, entry point [1] where this fact is reported and where the computer is subsequently blocked against further processing. In -35- the coded firmware, read from diskette, is decoded by the installation procedure where necessary and placed in memories -19-and -8-.

The CRC (Cyclic Redundancy Check) value is then computed individually per component of the protection means and checked with reference to the standard CRC value which is included in coded form in the protection firmware during manufacture thereof.

If the computed and the standard CRC of any of these components does not mutually correspond this means that modifications have been made to the firmware; this check is made in -36-.

If it is ascertained by the installation procedure in -36- that alterations have been made in the firmware or that the external information carrier does not fulfill the requirements set in -34-, a jump is then made to -39-, entry point [1] where this fact is reported and where the computer is subsequently blocked against further processing.

If all the conditions set in -36- result in a "Yes" condition, these different CRC values are then combined to one new CRC value which is stored in coded form -37- in the memory -8- for the purpose of checks which must take place during operation with the protection means.

In -38- the keys are then defined on the basis of which the information on the peripheral equipment such as for instance hard disc and tapes etc. has to be coded and encrypted. These are also stored in memory -8- in coded form. These keys ensure that the manner in which the information on such a medium is stored is no longer recognizable and also that the information is stored physically on the medium at a

BNSDOCID: <WO__9306542A1 I >

location other than is normally the case, with the result that this medium can only be further used with the protection means with which it was produced.

The removal of such a medium and incorporation thereof in another personal computer will come to nothing. Another personal computer will not recognize the medium and refuse to operate therewith since all information, and therefore all system information, is stored in code on that medium and at physical locations other than those anticipated by a non-protected personal computer. The keys which were used therefor are determined at random for each protection means at each installation.

It is also determined in -38- what the CRC of the system BIOS is and of eventual ROM extensions so that in the initialization phase of the basic protection it can be checked whether the system BIOS may have been substituted or other expansion boards have been added to the machine or modified without authorization.

A check is subsequently made in -39- whether problems have occurred during installation of the protection means.

If this is the case, all prior actions are cancelled and a message is given that errors have occurred and the machine is blocked.

Operation and advantages of the invention
(initialization figure 3)

The initialization stage of the installation procedure ensures automatic converting of the information on all the coupled and protected peripheral equipment so that after installation of the protection means at start-up of the computer the information thereon can be read. In -40- a first check is made as to whether this step has already been carried out earlier.

If that is the case an immediate jump is made to -45- entry point [2] and the procedure ended without anything being done. This a protection against performing this initialization phase twice, since this may take place only once.

A check is then made in -41- whether this action is performed by an authorized user and with the correct keys. If the keys have to be read from an external information carrier, there is a check as to whether this external information carrier fulfills the required specifications and if the General protection Key is present. If one of these conditions is not met, a jump is made to -45- entry point [3], this fact is reported and the computer is blocked against further processing. In the other case the processing continues with -42-.

A check is made in -42- whether the software of the protection means has been modified. This is done by comparing the CRC values coupled during manufacture to the different components of the protection means with the CRC value determined by the installation procedure in the course of installation -37-. If this results in the discovery that these two CRC values are not the same this means that something has been changed in the protection means and a jump is made to -45-. A message is given to this effect and the computer is blocked against further processing. If this test results in identical CRC values, processing proceeds with -43-.

In -43- the keys required for reading and writing of information from and to the peripheral equipment, such as for instance a hard disc, are taken out of memory -8-, decoded on

BNSDOCID <WO 9306542A1 | >

the basis of the General protection Key and placed in the memory -11-.

The actual conversion of the information from the old format to the new format takes place in -44-. This step is repeated until all information on the peripheral equipment is converted. Finally, a check is made in -45- whether errors have occurred during the initialization. If this is the case a message is given to this effect and the computer is blocked against further processing. If initialization has been error-free the installation procedure is ended by means of resetting the computer, at which point this will start as if it has been turned off and then switched on again.

A small portion of the hard disc is reserved by the initialization procedure to store information relating to the access check and the Encryption/Decryption, the rights to which are recorded per user. This reserving takes place only when these components have been installed and activated.

Operation and advantages of the invention
(removal of the protection means)

When the protection means is removed the installation and initialization process is in principle performed in reverse sequence. The coded information on the peripheral equipment is once again placed thereon in readable form and the plug-in card is restored to the state in which it was originally supplied so that it can be installed once again in another machine.

Operation and advantages of the invention
(basic protection figures 4a and 4b)

The basic protection comprises electronic circuits and software (firmware) which ensure that access to the machines and the information stored thereon such as software and information related thereto takes place with checks in a manner such that use thereof by unauthorized persons is not possible.

The software and the electronic circuits with which the monitored access to machines and information is realized by the basic protection is accommodated for the greater part in

BNSDOCID: <WO__9306542A1_I_>

a tamper-proof housing in which all the necessary checks are done by the protection means.

When the computer is started (initialized), see figure 4a, it is determined in memory -11- what is the state of the connections made between the protection means on the one hand and the FIRMWARE on the other during start-up of the computer. A check is also made during initialization whether the protection means is still in the state in which it was installed, in other words, whether any components have been changed which are of vital importance for the protection. Since the vital parts of the Basic Protection are included in the information carrier -8- in coded form, software must first be decoded. The decoded software is subsequently placed in memory -11-. The electronics in tamper-proof housing -25- also comprise a number of circuits which provide the security of the information recorded in the memories -8- and -11-.

The memories -8- and -11- can only be approached by following a stringent protocol wherein a number of conditions must be met with respect to program and in approaching electronic circuits. These memories are accommodated in the tamper-proof housing and are immediately blocked if they are not approached in accordance with the set requirements.

This means that if any of the conditions imposed by the electronic circuits is not fulfilled or if the conditions imposed by the firmware of the protection means are not fulfilled for approaching the memories -8- and -11- when these are read or written to, the information located in -11- is then immediately destroyed and the machine stopped.

It is impossible to determine from outside precisely what the conditions are which must be met and in which sequence these must be performed, as the tamper-proof housing consists of an opaque substance such as synthetic resin.

The conditions which have to be met cannot be simulated from outside as the protocol in the electronic circuits situated inside the tamper-proof housing ensures that determined series of instructions must be performed from a fixed location defined during installation. The structure of the electronic circuits inside the tamper-proof housing is such that attempts to bypass these protection means are

BNSDOCID: <WO 9306542A1 >

detected at all times and result in blocking of the machine. See also herefor **Operation and advantages of the invention** (hardware control).

Constructed on the plug-in card outside the hardware from which the basic protection is constructed is software whereof the operation will be elucidated with reference to figures 4a and 4b.

Figure 4a is a schematic representation of the initialization phase of the protection means which is activated when the machine is physically switched on.

A check is first made in -46- whether the protection means is installed. If that is not the case, a jump is made to -52- entry point [4] where this fact is reported and the user is instructed to install the protection means.

A check is made in -48- whether all firmware components are still in the state they were in at installation, as shown in figures 2 and 3, on the basis of the CRC values which are checked and stored at installation. If these elements are found to be in order, the external information carrier containing the key information and the PIN-code of the user are requested in -48- and -49- so that an identification check can be carried out as to whether the person who places the external information carrier -68- in the read/write unit -67- is indeed authorized to work with the information in this external information carrier. If an incorrect identification is entered for instance more than three times the external information carrier is then blocked against further use, which carrier can then optionally be unblocked for use again using special means, this subject to the type and options of the external information carrier.

If -48- and -49- are passed through successfully the key information is then read -50- from the card and a check is made whether the further information on the card is still valid. When the external information carrier is found to be invalid a jump is then made to -48-, entry point [5] where a correct external information carrier is requested once again.

If the external information carrier is valid, the key information is then stored safely in memory -11- inside the tamper-proof housing. A check is then made whether this is

the installation stage, or in other words, whether the software from -8- has already been placed in -11- in decoded form. If this is the case this step is then not performed, as otherwise the vital software included in memory -8- inside the tamper-proof housing is decoded on the basis of the just read keys and placed in memory -11- likewise situated inside the tamper-proof housing, whereafter the protection means is ready for its normal operations.

The normal operations of the basic protection are shown schematically in figure 4b. It can be seen in -53- that from a number of points inside the equipment and software this process can be set into motion, namely:

- when something is entered from the keyboard,
- when a request is made to write information to one of the peripheral machines or to read information from one of the peripheral machines,
- when an interrupt is forced by the motherboard by means of the timer installed thereon, the so-called timer tick.

A check is first made in -54- whether a valid external information carrier -68- is still present in the read/write unit -67- and whether this has not for instance been removed or exchanged in the meantime. If this is indeed the case, a jump is made to -48-, entry point [5] where a request is then made to place an external information carrier -68- in the read/write unit -67- and to enter the associated PIN-code. If this is found to be in order, a check -55- is made as to whether in the meantime anything has been altered on the machine and the software and/or firmware of the protection means and other ADD-ON Boards. Should this be the case a jump is then made to -52-, entry point [4] where the machine is blocked against further processing. If this is also found to be in order, the request is then dealt with or transmitted, this subject to the request, and the normal process is resumed -57-.

As the protection means intervenes in all vital functions of the machine that are required to enter and store information in the machine, it is impossible to work with the machine outside the protection means.

BNSDOCID: <WO 9306542A1 >

Nor can work be done with the stored information on the machine as this information cannot be read without the protection means because this information is stored in coded form and can only be decoded with the protection means and the associated keys.

Operation and advantages of the invention

(access control and encryption/decryption figure 5)

The software for the Access Control and Encryption/Decryption of the information on the peripheral equipment, for instance hard discs, which are coupled to a machine are a separate component of the protection means. This component provides the coding and decoding of information coupled to user rights and the physical access to these user rights.

This coding of information takes place together with the coding and decoding of the basic protection and offers the possibility of making a physical distinction on one machine between the different authorized users and the information relating thereto and as an additional obstacle that must be cleared when anyone wants to gain unauthorized access to this information.

With the access control can be determined which user or users have access to particular software and information and whether this information and/or software has to be stored in coded form. The operation thereof can be described as follows:

The access control functions per se independently of operating systems, with the understanding that per operating system a function is created independently of the protection means with which it is possible to transfer the operating system-associated information to the protection means in a uniform, non-operating system-related format, whereby the actual checking with respect to granting of access to information can be further regulated irrespective of the system. Another advantage here is that when new operating systems are introduced it can suffice to produce a small piece of software for this new operating system which converts the information individual to this operating system to the uniform format with which the protection means works.

A small portion of the hard disc is reserved for the access control. On this portion of the hard disc is stored in coded form per user whether a user has access to a determined piece of information that is held on the peripheral equipment of the machine. The rights of each user are coded using a unique key, which means that user "A" with knowledge of his individual user key could only decrypt his own information but never the information held for user "B".

If in -56- it is detected that the access control and encryption/decryption functions are active, a jump is made to -58-, entry point [8]. Here a check is made whether the external information carrier -68- is present in the read/write unit -67- and is still intact. Should this not be the case, the protection means then requests placing of the external information carrier -68- in the read/write unit -67- and entry of the associated user key. If the above is not the case the protection means checks -59- whether all connections are still intact and whether all checks can be performed. If this is not the case, the machine is blocked. If all checks proceed properly, a check is made as to whether the user has rights of access to the information that he or she wishes to use -60-. If this is the case, the information is released to the user.

Should this user not have any right to approach this information, access thereto is then refused and the information is not released by the protection means.

Operation and advantages of the invention
(encryption/decryption algorithms)

For key control and coding and decoding of information use can be made of two different algorithms both having a specific function within the protection means. For the distribution of protection keys with which the information can be coded and decoded, use can for instance be made of the RSA algorithm, while the coding and decoding of the actual information can be done with the DES algorithm.

A description of the RSA algorithm can be found in

BNSDOCID: <WO 9306542A1 I >

"A method of obtaining digital signatures and public-key cryptosystems" written by R.L. Rivest, A. Shamir and L. Adleman.

A description of DES is included in the "Federal Information Processing Standard", No. 46, US National Bureau of Standards, 15 January 1977.

Since the RSA algorithm operates with a public and a private key-pair this is excellently suited for distributing in safe manner keys with which information must be coded and decoded, wherein the key with which new keys for coding and decoding information can be distributed is only known to the security controller.

The RSA key required to be able to decode the DES keys for the purpose of coding and decoding of information is known only to the users of the protection means. These RSA user and controller keys are defined at installation and stored in coded form in memory -8- situated inside the tamper-proof housing.

For coding and decoding of information use is made of a second wholly different algorithm, such as for instance DES. Using the DES algorithm information can be coded and decoded with one and the same key. The working with the secret keys is done only in memory situated inside the tamper-proof housing and is never to be found in normal memory where it would be accessible to anyone.

Only after the coded DES key is situated in the memory inside the tamper-proof housing is this key decoded on the basis of the RSA key likewise situated in that memory. Only then can decoding of information be carried out. The distribution of keys from an external information carrier to the memories inside the tamper-proof housing is thus protected, since the real key only becomes known in that memory.

*****

BNSDOCID: <WO 9306542A1 I >

Claims

1. Computer system comprising a computer, for instance a personal computer (PC) with protection means which protect the software and information present in the computer against unauthorized use,

characterized by

a plug-in card for placing in a connecting device forming part of the computer and comprising:

a tamper-proof housing;

a control circuit;

a switch controlled by this control circuit and having a first and a second position;

a volatile memory in which is included information in software form indispensable to the operation of the system, wherein in the first position the switch connects the memory for feed to an energy source and in the second position the switch interrupts the connection between the energy source and the memory, wherein the control circuit is adapted for detecting possible non-authorized actions, wherein in the first position the memories can be made available in specific conditions for writing or reading of information, and wherein in the second position the detection means carry the switches or a part thereof from the first position to the second position when non-authorized actions are detected, wherein the memories are disconnected from the energy supply with the result that the vital information in these memories is instantaneously erased and/or these memories are made inaccessible for further external actions such as read and write commands until the system is switched off and subsequently switched on again, wherein the disconnection of the memories from their energy source and making these memories physically inaccessible by causing the switches to move into the second position

BNSDOCID: <WO 9306542A1 I >

can also take place under the influence of the software present in these memories when variations are detected relative to the protection rules included in the system.

2. System as claimed in claim 1, **characterized in that** the energy supply of the memories is realized by means of these electronic switches in addition to the physical access to these memories, wherein the first position and the second position of the electronic switches represent respectively a closed and an open switch.

3. System as claimed in claim 2, **characterized in that** the switches are actuated by detection means which consist per se of electronic circuits which have the object of setting imperative conditions for access of the memories of which the energy supply and the physical access is controlled by the switches coupled to these detection means in a manner that approach to these memories cannot be realized in any way whatever other than in accordance with the protocol imposed for this purpose.

4. System as claimed in any of the foregoing claims, **characterized in that** the detection means are provided with inputs for receiving externally supplied information and commands and with outputs for placing the switches in the second position in response to the supplied information and operations not corresponding with the protocol imposed by the electronic detection means.

5. System as claimed in any of the foregoing claims, **characterized in that** the detection means are coupled to the address inputs of the memories accommodated on the plug-in card in order to place the switches or a part thereof into the second position in response to variations in the required conditions relating to predetermined series of addresses and the contents incorporated therein, wherein both the addresses and the contents of the memory at these addresses and the sequence in which these memory locations are approached determine the protocol that is checked by these detection means.

6. System as claimed in any of the foregoing claims, **characterized in that** the vital memories and switches and

detection means are accommodated in an opaque tamper-proof housing which is per se provided with detection means, electronics and an individual energy source which make it impossible to open this housing without irretrievably damaging the electronic circuits accommodated therein.

7. System as claimed in any of the foregoing claims, **characterized in that** software is arranged thereon in information carriers to protect the machines and information against unauthorized use, which, with respect to the vital parts of this software and the information relating thereto, is accommodated in memories situated inside the tamper-proof housing and which can only be approached by following a stringent protocol.

8. System as claimed in any of the foregoing claims, **characterized in that** the memories arranged thereon for holding the firmware and the coded protection keys are volatile memories, with the understanding that in the voltage-free state these act as non-volatile memory, with the characteristic that alterations in the information included in these memories can take place in electronic manner without alterations having to be made therefor on the plug-in card itself or components having to be exchanged.

9. System as claimed in any of the foregoing claims, **characterized in that** on the plug-in card software and information can be loaded into memories which have the object of coupling the use of information, in whatsoever form, on peripheral equipment of the computer plug-in card to authorization by means of identification prior to it being possible to make use of this information, wherein this software also ensures that the storage of information on the peripheral equipment takes place in a manner such that this information is placed physically at other addresses in relation to a different computer and these can only be determined by the software of the plug-in card and that this information is coded in accordance with a specific algorithm, for instance DES, prior to being stored on the peripheral equipment.

10. System as claimed in any of the foregoing claims, **characterized in that** new versions of the protection firmware

BNSDOCID: <WO 9306542A1 | >

can be distributed on a normal medium, for instance diskette, and can be installed by authorized users by means of special software developed for this purpose without components on the plug-in card having to be exchanged herefor or modifications having to be made to the equipment, wherein the use of volatile or non-volatile memory has no influence on the functionality of the protection means itself other than on the management aspect in respect of the distribution of new versions thereof.

11. System as claimed in any of the foregoing claims, **characterized in that** for the operation of the protection means no claim is made on functionalities of the equipment normally available to the user such as for instance working memory and terminals for external or internal equipment, with the exception of the address space required to make the electronics of the plug-in card accessible to the machine in which it is placed.

12. System as claimed in any of the foregoing claims, **characterized in that** an external read/write unit can be connected thereto for reading and writing information in an external information carrier with the object of obtaining an unambiguous identification of users and can serve as secured storage for user keys and general protection information.

13. System as claimed in any of the foregoing claims, **characterized in that** the plug-in card functions as an extension to the functionality of the machine in which it is arranged and is not an extension of the functionality of the operating system required to work with the machine.

14. System as claimed in any of the foregoing claims, **characterized in that** the plug-in card is provided with electronic circuits which have the object of disturbing the information being exchanged between the plug-in card and the machine over the address and data bus at random moments with random data patterns which makes considerably more difficult if not impossible the interpretation of the information being exchanged or approached.

15. System as claimed in any of the foregoing claims, **characterized in that** if it is electronically constructed in a different way in respect of functionality and method it can

operate in any machine that is provided with a processor and firmware, such as for instance normal data communication work stations.

16. System as claimed in any of the foregoing claims, **characterized in that** the plug-in card can be embodied without determined electronic protection means, wherein the degree to which protection is required can play a significant part, or can be embodied with electronic components of another brand or type but which ultimately lead to essentially the same result, wherewith the method of the protection means is not detracted from per se.

17. System as claimed in any of the foregoing claims, **characterized by** means to protect software against unauthorized copying, wherein one and the same copy protection can function for all software, wherein no intervention by the user is necessary and no external auxiliary means have to be used other than the protection means in order to be able to work with the protected software.

18. System as claimed in any of the foregoing claims, **characterized in that** when an unauthorized action is detected the voltage source physically destroys the memory present on the plug-in card.

19. System as claimed in claim 18, **characterized by** a voltage multiplier connected to the voltage source.

20. System as claimed in any of the foregoing claims, **characterized in that** it is equipped with electronics which, independently of other electronics and software, couples by means of a timer a time limit to the approaching of the protection means, wherein in response to this time control not being observed the electronic switches are placed in the second position, wherein the independent timer effectively functions as an independent monitoring circuit which cannot be influenced from outside.

21. System as claimed in any of the foregoing claims, **characterized in that** cyclic checks are made as to whether the firmware components are in the state recorded at installation of the plug-in card, and in the case of variation the equipment is blocked.

22. System as claimed in any of the foregoing claims, **characterized in that** this blocks itself in the case of non-authorized operations and can only be unblocked by turning off and switching on the computer.

*****

BNSDOCID: <WO 9306542A1 >

FIG. 1

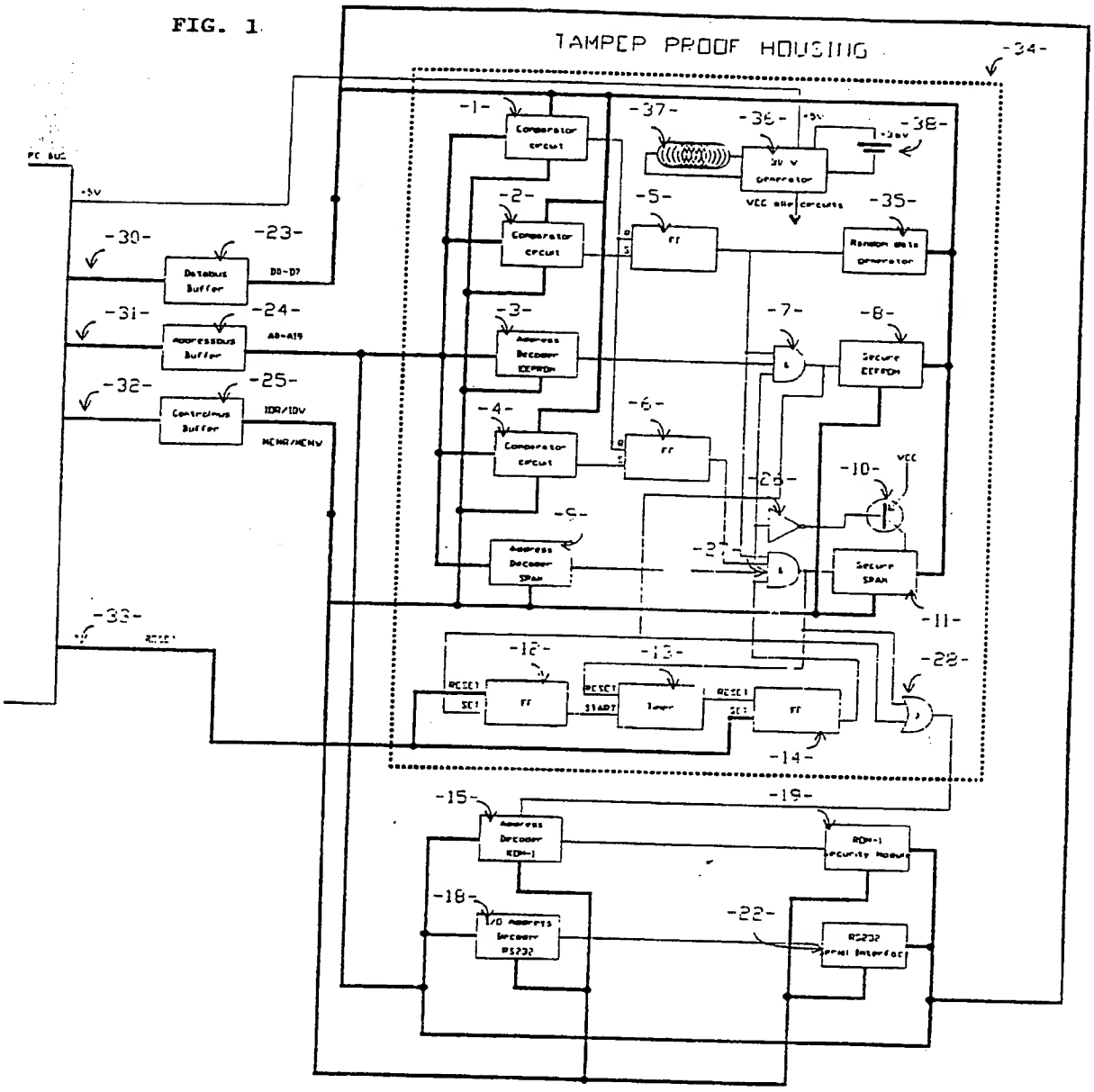
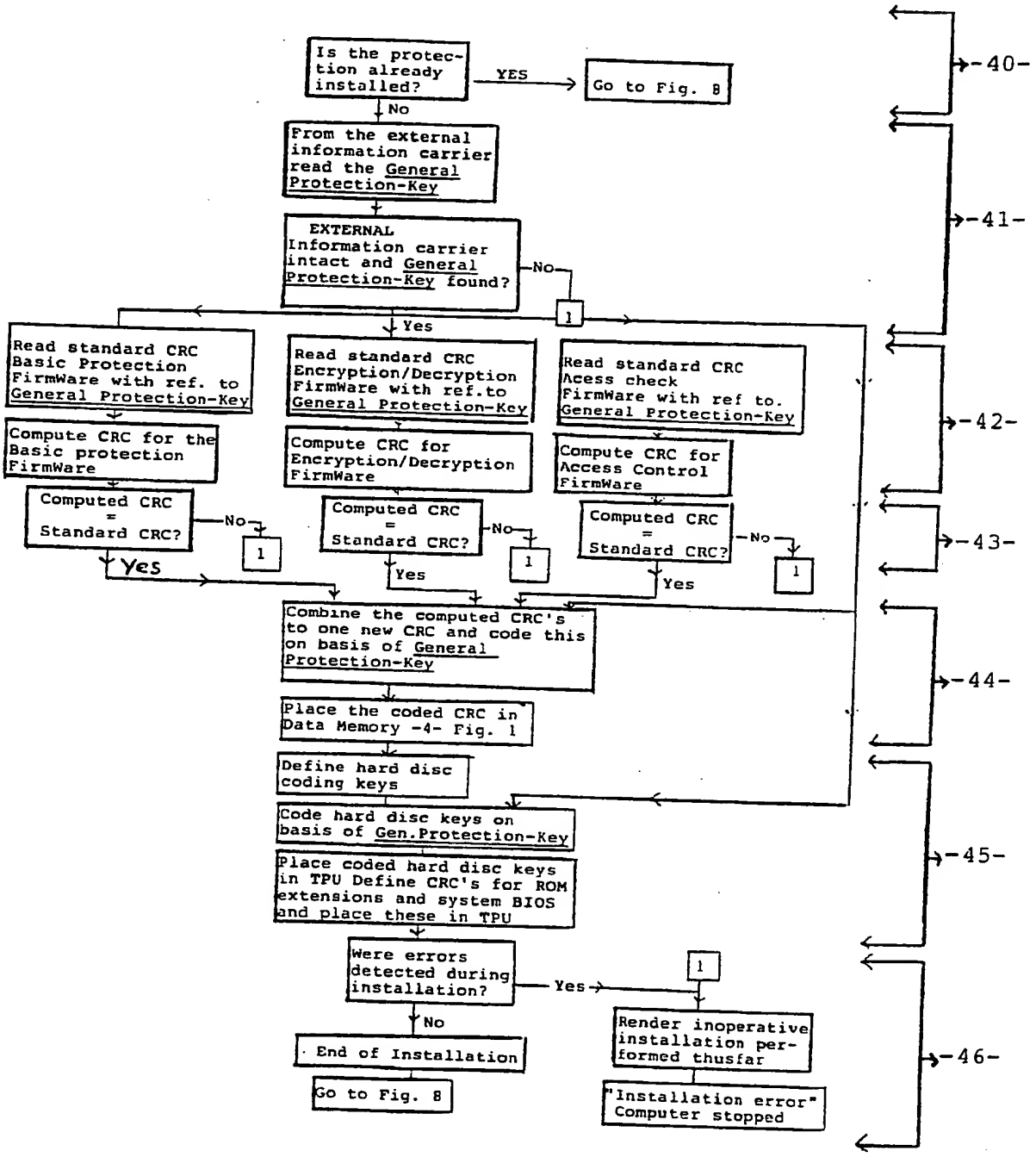

TAMPER PROOF HOUSING
-34-
-1-
-2-
-3-
-4-
-5-
-6-
-7-
-8-
-9-
-10-
-11-
-12-
-13-
-14-
-15-
-18-
-19-
-22-
-23-
-24-
-25-
-26-
-27-
-28-
-30-
-31-
-32-
-33-
-35-
-36-
-37-
-38-

FIG. 2

Schematic representation installation phase



BNSDOCID: <WO 9306542A1 I >

FIG. 3

Schematic representation initialization phase

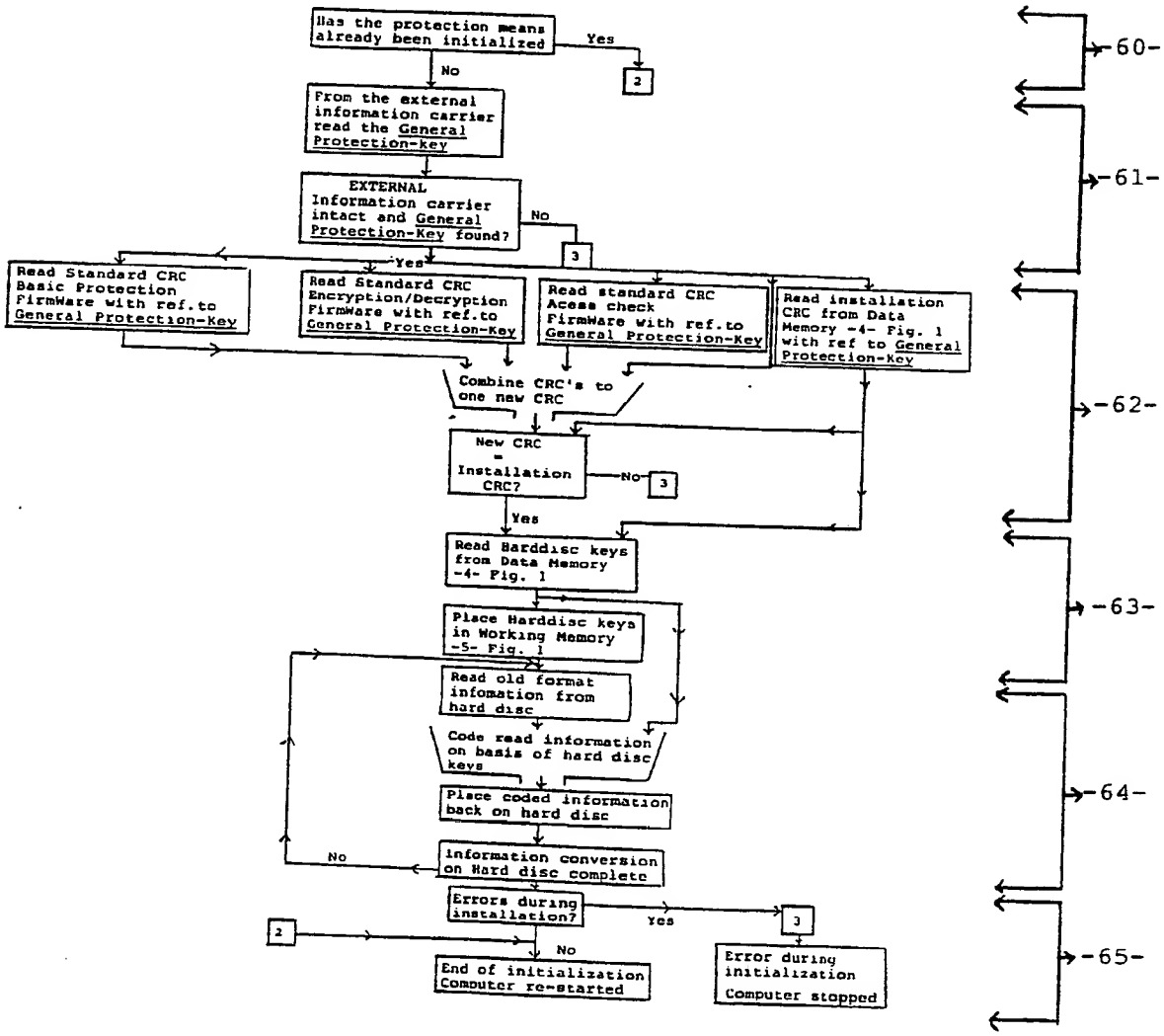
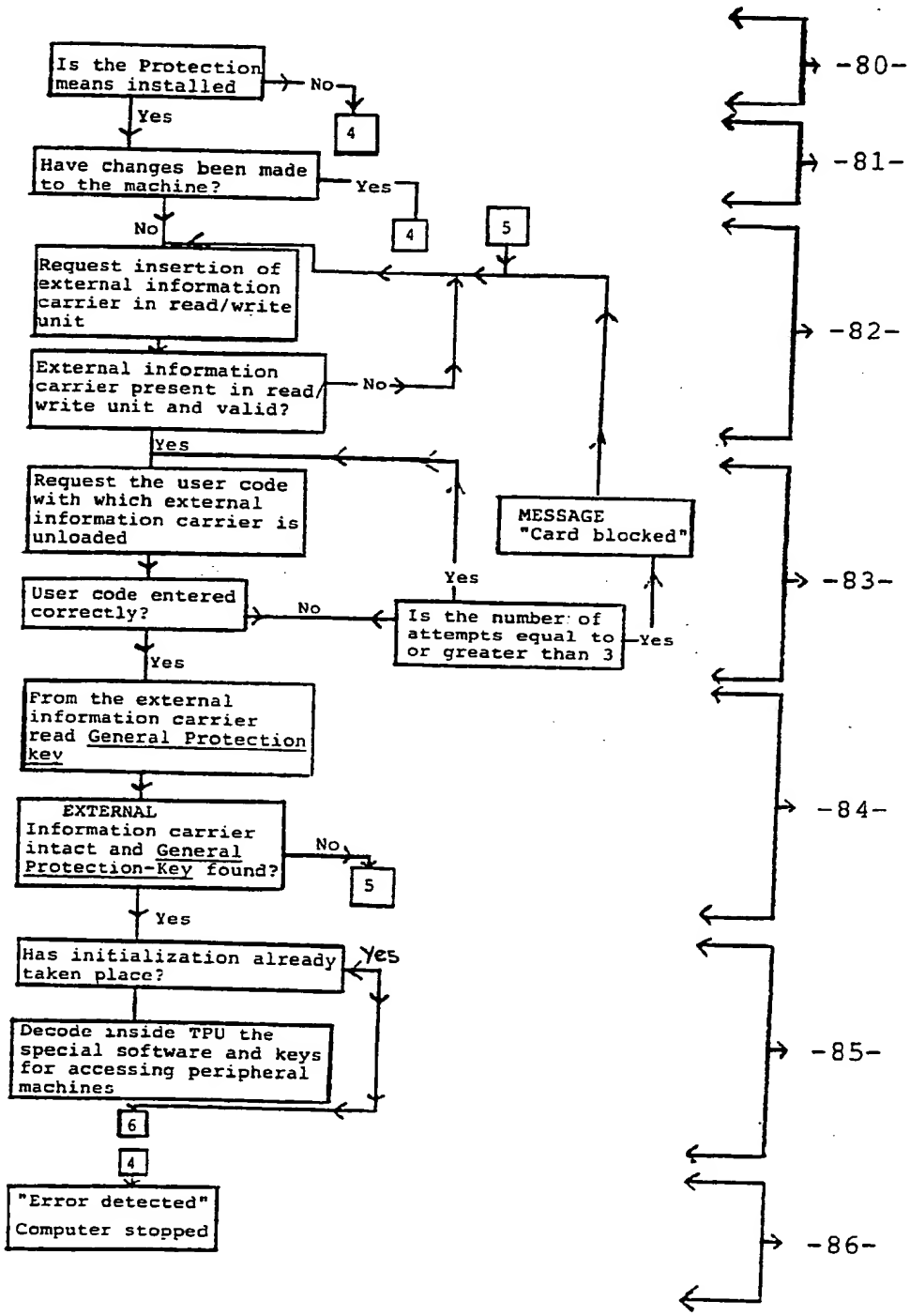


FIG. 4a

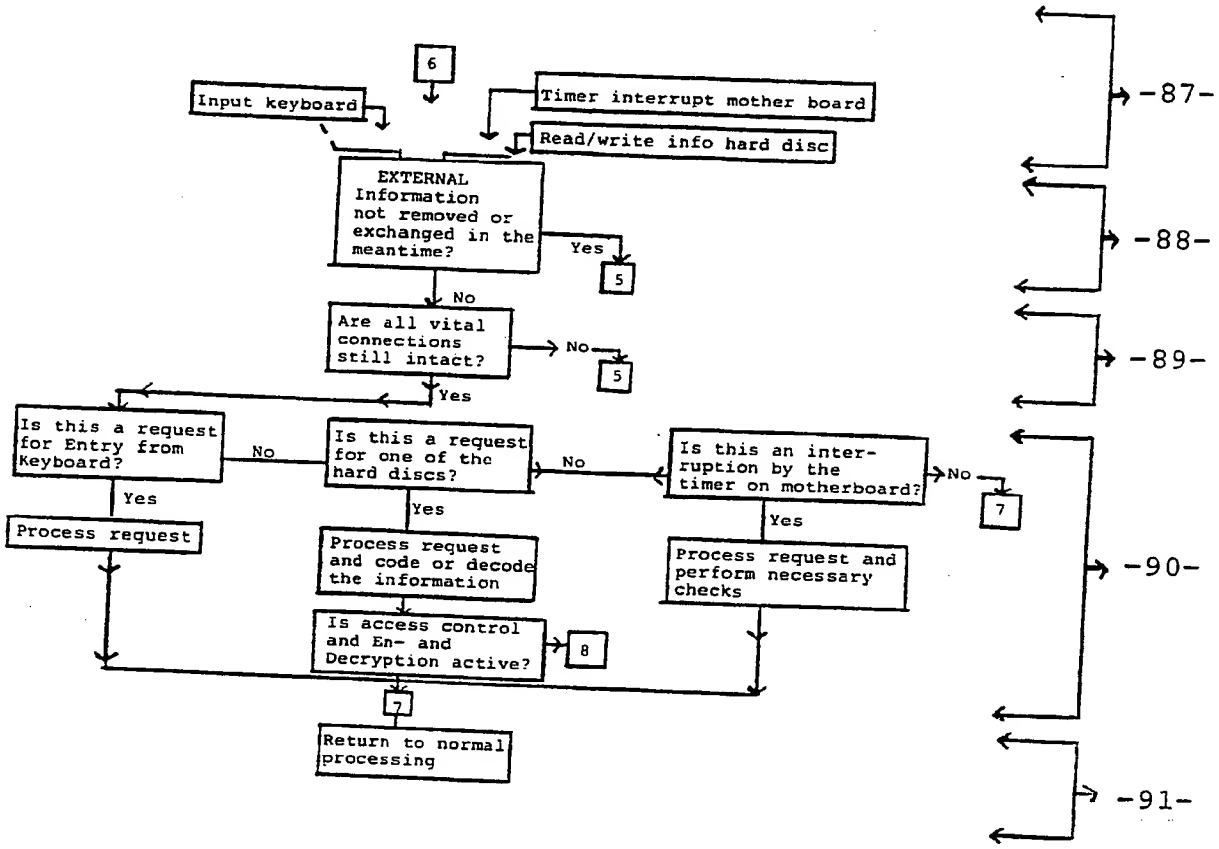
Schematic representation BASIC PROTECTION initilization



BNSDOCID: <WO___9306542A1_I_>

FIG. 4b

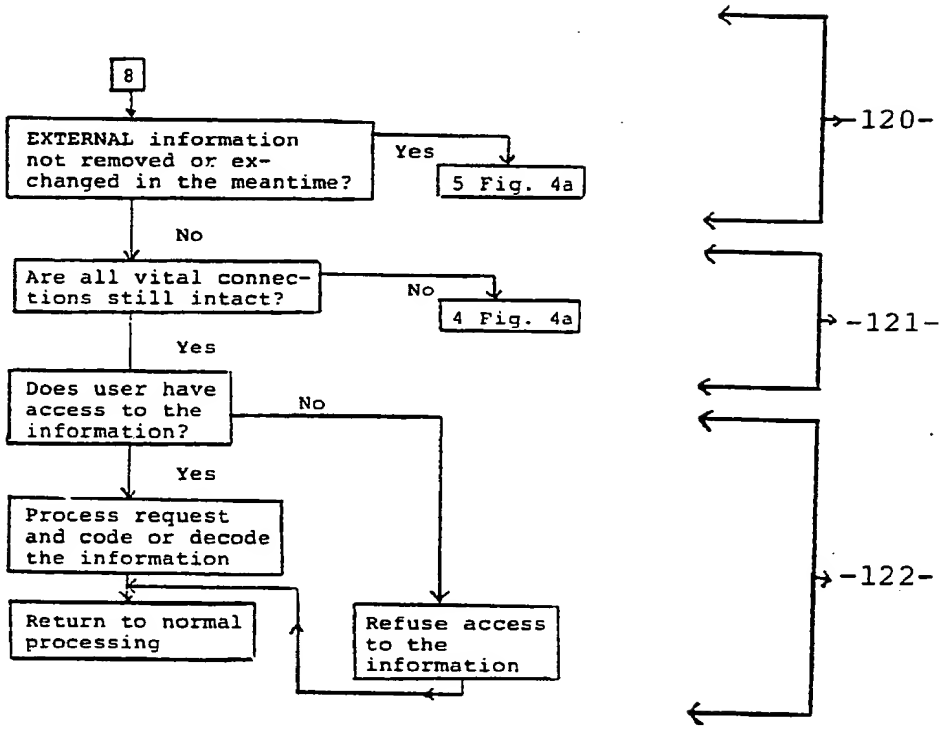
Schematic representation BASIC PROTECTION



BNSDOCID: <WO 9306542A1 I >

FIG. 5

Schematic representation ACCESS CONTROL AND ENCRYPTION/DECRYPTION



BNSDOCID: <WO___9306542A1_I_>

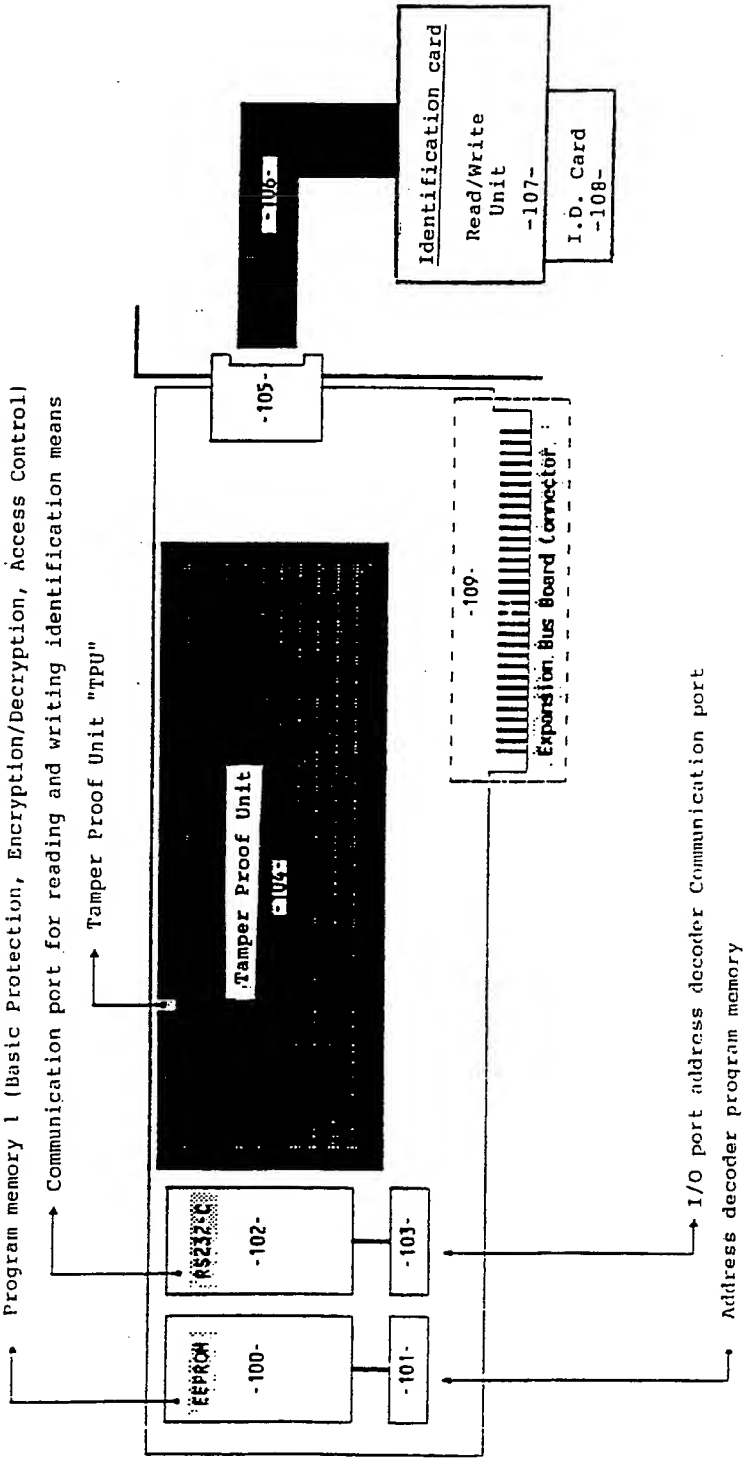


FIG. 6

BNSDOCID: <WO 9306542A1 I >

INTERNATIONAL SEARCH REPORT

International Application No PCT/NL 92/00161

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all)[6]

According to International Patent Classification (IPC) or to both National Classification and IPC

Int.Cl. 5 G06F1/00

II. FIELDS SEARCHED

Minimum Documentation Searched[7]

Classification System	Classification Symbols
Int.Cl. 5	G06F

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched[8]

III. DOCUMENTS CONSIDERED TO BE RELEVANT[9]

Category °	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No.[13]
A	EP,A,0 266 748 (IBM) 11 May 1988 see column 19, line 28 - column 20, line 48 see column 22, line 35 - column 24, line 20; figures 1,6	1-2,6, 8-11,13, 15-18,20
A	EP,A,0 142 013 (MARTE) 22 May 1985 see page 14, line 3 - line 11 see page 19, line 5 - line 13; figures 6-10	1-2,6,18
A	US,A,4 716 586 (BAUER) 29 December 1987 see column 2, line 3 - line 41; figure 1	1,3-5

° Special categories of cited documents : [10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
28 DECEMBER 1992	07. 01. 93
International Searching Authority	**Signature of Authorized Officer**
EUROPEAN PATENT OFFICE	MOENS R.A.

Form PCT/ISA/210 (second sheet) (January 1985)

BNSDOCID: <WO__9306542A1 I >

ANNEX TO THE INTERNATIONAL SEARCH REPORT ON INTERNATIONAL PATENT APPLICATION NO. NL 9200161 SA 65170

This annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The members are as contained in the European Patent Office EDP file on 28/12/92
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP-A-0266748	11-05-88	US-A- 4817140	28-03-89
		EP-A- 0268139	25-05-88
		JP-B- 3032813	14-05-91
		JP-A- 63127334	31-05-88
		US-A- 5109413	28-04-92
		JP-C- 1630817	26-12-91
		JP-B- 2060009	14-12-90
		JP-A- 63128434	01-06-88
EP-A-0142013	22-05-85	None	
US-A-4716586	29-12-87	None	

BNSDOCID: <WO 9306542A1 | >